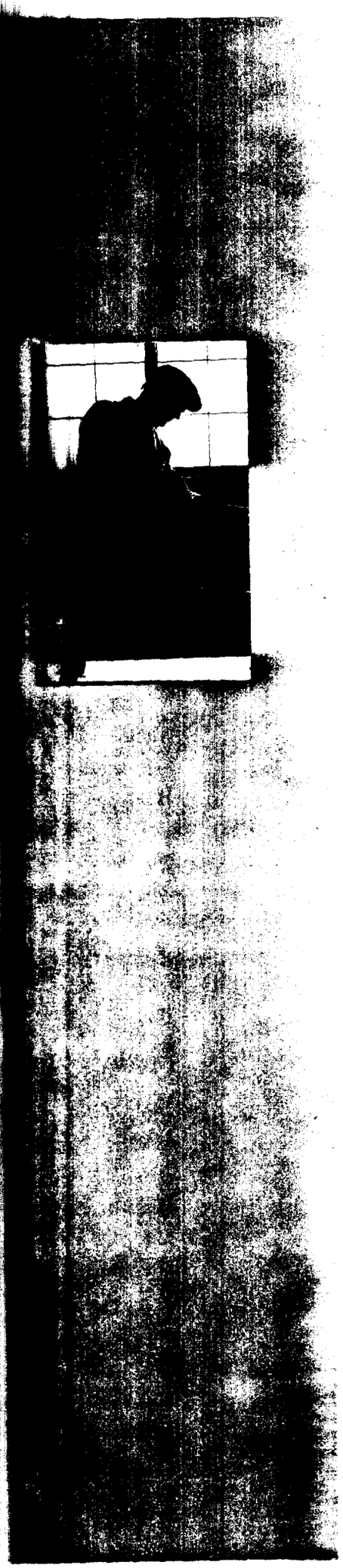
For small businesses, Remote Toll Fraud can be a big problem.

If you think Remote Toll Fraud only strikes big companies, think again! Toll fraud *does* happen to small companies – and *could* happen to yours.

Imagine this: One weekend when your office is closed, you get a call from AT&T Corporate Security. They've noticed an unusual pattern of calling from your number and sure enough, it turns out that someone has figured out a way to call in on one line and get transferred to a line out.

Thanks to *AT&T NetPROTECT™ Basic Service* – provided to you automatically – you are able to put a stop to the fraud before it does your business serious harm. But when it comes to Remote Toll Fraud, every minute can cost you plenty. And what would have happened if you weren't around when AT&T Corporate Security called?

That's why you should order *AT&T **NetPROTECT™** Plus Service.* For a one-time set-up charge of $25 and a monthly fee of only $10 per location, AT&T provides enhanced monitoring. In addition, the ***NetPROTECT™*** Service Center keeps a list of three different contacts in your firm to notify. If Corporate Security can't reach you, they'll reach someone else. And, if you choose, you can authorize AT&T to block all outgoing calls the minute they suspect trouble. After all, your business is at stake.



AT&T NetPROTECT™ PLUS SERVICE: AN EXTRA MEASURE OF PROTECTION FOR ONLY $10 A MONTH.

Available by subscription, ***AT&T NetPROTECT™ Plus Service*** offers extra protection to *AT&T Business Long Distance Service* customers who have two or more lines and the ability to connect an incoming line to an outgoing line.

For a one-time installation charge of $25 per location – limited to $500 for multiple locations – and a nominal per-location fee of $10 a month, *Plus Service* provides all the benefits of ***AT&T NetPROTECT™*** *Basic Service* plus these additional benefits:

- Intensified monitoring. By looking at the combined activity of all incoming and outgoing lines at a customer location, AT&T warning thresholds are reached at lower levels.
- Enhanced notification. AT&T Corporate Security will register the names of three (3) contact numbers covering 24 hours a day, 7 days a week. Customer fax and/or ATTMAIL numbers will also be registered, in case none of the customer contacts can be reached.
- Custom call-record analysis. To avoid unnecessary notification to the customer, AT&T will refer to the customer's international calling patterns after determining generally suspicious activity.
- Call blocking on request. If fraud is suspected, AT&T will, at the customer's written request, block all outgoing AT&T calls.

AT&T NetPROTECT™ ADVANCED SERVICE: LIMITING CUSTOMER LIABILITY.

AT&T NetPROTECT™ *Advanced Service* provides a higher level of protection because it:

- Caps the customer's initial liability at $25,000 per location for each incident during the period prior to notification of suspected covered PBX Remote Toll Fraud.*
- Waives customer liability for two hours after notification.
- Reduces customer liability for covered PBX Remote Toll Fraud by 50% if the customer detects toll fraud before AT&T and notifies AT&T Corporate Security.**

To qualify for this service, a customer must have: *AT&T Business Long Distance Service*; *AT&T Domestic 800 Service* providing at least 30% of total inbound service; a PBX or Single Keypad System; Access Limitation to Remote Ports; Call Accounting; Protect DISA Password; and a List of Originating Telephone Numbers provided to AT&T. Certain additional conditions may apply. This is provided to AT&T business customers for an additional service charge.

* PBX Remote Toll Fraud excludes certain forms of calling, such as operator handled and cellular calls.

** Up to the first $25,000.

DON'T BE CAUGHT IN THE MIDDLE OF A TOLL FRAUD FIASCO.

Could this scenario happen to you?

You're responsible for telecommunications in a growing mid-sized company. In fact, recently you had *AT&T Domestic 800 Service* installed. Because the company is investing heavily in its future growth, budgets are tight – and controlling expenses is a high priority.

Suddenly, your company gets "blitzed" with fraudulent phone calls. Thanks to *AT&T **NetPROTECT**℠ Plus Service*, AT&T Corporate Security catches on to it quickly. But still, you can't believe how much is run up in a short period of time. It's enough to turn what would have been a profit for that quarter into a loss.

Now suppose you had ordered *AT&T **NetPROTECT**℠ Advanced Service.* Instead of being liable for several hundred thousand dollars, your liability for the covered Remote Toll Fraud occurring before detection is capped at $25,000. Plus, AT&T gives you two liability-free hours after detection to correct the problem.

Bottom line: Your company shows a profit after all. And you show your company some foresighted thinking.

AT&T NetPROTECT℠ PREMIUM SERVICE: THE HIGHEST LEVEL OF AVAILABLE PROTECTION.

AT&T NetPROTECT℠ Premium Service provides the same benefits as *Advanced Service*, including no customer liability for covered PBX Remote Toll Fraud for two hours after notification of fraudulent calling activity. In addition, it:

- Reduces initial customer liability to zero for covered PBX Remote Toll Fraud, including international and *AT&T Domestic 800 Service* calls, during the period prior to AT&T notification.

To qualify for this service, a customer must meet all the requirements of *AT&T NetPROTECT℠ Advanced Service* and must have: *AT&T Domestic 800 Service* providing 100% of all inbound service, a longer Protect DISA Password, and an AT&T Security Review. Certain additional conditions may apply.

AT&T NetPROTECT℠ HELPS LARGE COMPANIES SPEND A SMALLER TARGET FOR TOLL FRAUD.

If you're the telecom manager for a large corporation, you probably know how those telephone hackers think. They look at your complex phone system and see more ways to beat it. They look at your multiple locations and see more areas of "opportunity." And because your telecommunications arrangements may be quite complex, they figure their fraud will go unnoticed for some time.

That's one excellent reason to choose AT&T for all your domestic and international, outbound and inbound, switched and dedicated service. Not only do you get the quality of AT&T, but you also have the added value and protection of the *AT&T NetPROTECT℠ Family of Services.*

AT&T Corporate Security professionals will work with you to help assure you have the right package of round-the-clock monitoring and liability coverage at all your locations. And when your toll-free inbound service is 100% *AT&T Domestic 800 Service*, you're eligible for *AT&T NetPROTECT℠ Premium Service.* That means *no liability* whatsoever for covered Remote Toll Fraud occurring prior to notification.

When it comes to providing toll-fraud protection, AT&T is unsurpassed.

FOR MORE INFORMATION, CONTACT YOUR AT&T ACCOUNT REPRESENTATIVE OR CALL TOLL FREE: **1 800 NET SAFE.**

A representative from AT&T Corporate Security can answer your questions and provide additional details on how to safeguard phone systems with *AT&T NetPROTECT℠ Services* – The Early-Warning System Against Costly Toll Fraud.

AT&T. Far and Away. The Best in the Business℠.

News Release

For further information:

Ellen Sundl
908-221-5017 (office)
201-543-2236 (home)

Mark Siegel
908-221-8413 (office)
201-366-6863 (home)

FOR RELEASE MONDAY, FEBRUARY 3, 1992

(BASKING RIDGE, N.J.) -- AT&T and Consumer Alert, a nationwide, nonprofit consumer organization based in Washington, D.C. and Modesto, Calif., today launched a consumer education campaign to help older Americans avoid becoming victims of telephone fraud.

Although telephone con artists prey on people of all ages and lifestyles in what telephone industry experts estimate is a $1 billion a year ripoff, consumers over the age of 60 are often targets.

The consumer education effort will focus on building awareness of telephone scams and ways to combat them. Some 6,000 senior centers have been sent posters, information for dissemination through local newsletters and free brochures. The campaign will be supported by public service announcements and print advertising underwritten by AT&T.

"The best defense against telephone fraud is an educated consumer," said Barbara Keating-Edh, president of Consumer Alert. "If people understand how telephone scams work they can avoid becoming victims."

(more)

In one common fraud scheme, sometimes called the "Just Say Yes" scam, a thief impersonating an investigator calls the victim at home and asks for cooperation in a telephone company investigation. The victim is then asked to help catch a criminal (or fix a service problem) by accepting charges for a series of collect calls.

The imposter assures victims they won't be billed for the calls and, in some cases, may promise substantial credit or cash payment as an incentive. If a customer is reluctant to participate, the imposter may threaten to cut off the victim's phone service.

Contrary to what they may be told by con artists, consumers are responsible for charges they willingly accept. What's more, because many of these charges are costly to collect, long distance companies lose millions of dollars to fraud every year. That drives up the cost of doing business and, as a result, all of the company's customers are victimized.

AT&T also advises consumers to be on the lookout for thieves intent on stealing their telephone calling card number. Some card number thieves frequent public places such as bus, train and airline terminals, eavesdropping or spying on unsuspecting callers to obtain their calling card numbers. Others will call victims at home, using a variety of phony excuses to trick a customer into revealing a calling card number.

(more)

Avoiding and Reporting Telephone Fraud

Here are some tips offered by AT&T to help consumers avoid becoming victims of telephone fraud:

- If you receive a call from anyone claiming to be a phone company or law enforcement investigator asking you to accept charges or to reveal your calling card number, hang up immediately. No legitimate representative would ever ask you for such cooperation or information.

- If you suspect you are a victim of a telephone scam aimed at getting you to accept charges for telephone calls, report it immediately by calling the number for billing inquiries that appears on your phone bill.

- If you suspect that your telephone calling card has been lost, stolen or otherwise compromised, report this immediately to your long distance company. The company will cancel your calling card number immediately and issue you a new card. If you are an AT&T customer, simply dial 1-800-CALL ATT.

- Make every effort to protect your calling card number. Do not use your card as identification when making purchases and make sure no one can see you keying in your calling card number or overhear you reading the number to an operator. Whenever possible, use a public phone that reads your calling card automatically.

(more)

To obtain a free booklet on telephone fraud, call AT&T toll-free at 1-800-222-0300, extension 273.

# # #

AT&T

News Release

For further information:

Jon Mellor, AT&T
908-221-5017
908-874-8964 (home)

AT&T SAYS 'TIS THE SEASON TO BE CAREFUL WITH CALLING CARDS
FOR RELEASE TUESDAY, NOVEMBER 30, 1993

BASKING RIDGE, N.J. -- AT&T warns consumers that calling-card-number thieves love the holiday season, too. As shoppers and travelers use their long-distance calling cards in malls and transportation hubs, they should be aware that their calling-card numbers are at the top of some criminals' wish lists.

Consumers should protect their calling cards as they would protect credit cards or cash. AT&T offers the following tips:

o When entering calling-card numbers on public phones, obscure the card, keypad and hand movements from prying eyes. If possible, use a phone that reads the magnetic strip on the back of your calling card. Most AT&T public phones are equipped with a card-swipe or card-insert feature.

- more -

o A criminal will pretend to have a conversation on one public phone to hear what's being said at the next phone. If you must read your card number to an operator, speak softly to avoid being overheard.

o Customers should call their calling-card providers to learn what safeguards those companies offer. For instance, AT&T Personal Choice Calling Card customers can easily memorize their card numbers, so they don't need to carry or expose their cards to place calls. And all AT&T calling-card customers can put restrictions on their cards that prevent the cards from being used for international calls--the favorite use of calling-card thieves.

o Report stolen calling cards or suspicion of fraud to your long-distance company immediately. The company will cancel the calling-card number and issue a new card to you. AT&T Calling Card customers should call 1-800-CALLATT.

For a free brochure detailing these tips and other ways for consumers to protect themselves, call AT&T on 1-800-851-0439

# # #

News Release

For further information:

For more information:
David Bikle
201-644-7052 (office)
201-871-0104 (home)

FOR RELEASE WEDNESDAY, DECEMBER 8, 1993

AT&T WARNS BUSINESSES: "HOLIDAY EFFECT" MEANS INCREASED TOLL FRAUD

Basking Ridge, N.J.-- AT&T urges businesses to guard against increased risk of toll-fraud attempts by hackers, or toll-call thieves, during the upcoming holiday season. Last year nationwide toll-fraud attempts increased by about 50 per cent during the Christmas week. Hackers "break into" PBX's or voice-mail systems, obtain passwords or access to outside lines, and then sell or use the information to make illegal international phone calls.

Toll fraud cost American businesses more than $2 billion in 1993.

"Hackers count on being able to steal calls undetected while businesses are closed during a long holiday weekend," says Larry Watt, director of AT&T's Toll Fraud Prevention center. "'Tis the season to be wary."

- more -

AT&T suggests several steps businesses can take to protect against phone fraud:

o Program PBX's to block outgoing calls to foreign countries during the hours the business is closed. Also consider blocking remote access into PBX and voice-mail systems both after hours and throughout the holiday weekends.

o Deactivate or restrict call transfer out of voice mail and auto-attendant systems.

o Institute a regular schedule for changing access codes and passwords, and always delete unused codes.

o Enroll in a fraud-prevention program that will call the customer whenever suspicious calling patterns are detected -- even in the evening and on weekends -- so the long-distance carrier can quickly block further illegal outgoing calls. AT&T monitors virtually all of its business customers' calls 24 hours a day, and its NetPROTECT(SM) Services include notification of fraud attempts even at night and on weekends.

For example, with NetPROTECT Plus Service a business can designate three people and their reach numbers after work hours, so that AT&T can notify the representative and work with him or her to stop the fraud quickly.

AT&T is the industry leader in helping companies to prevent toll fraud. Businesses that want more information on preventative measures can request AT&T's free booklet, "Tips on Safeguarding Your Company's Telecom Network," by calling 1-800-NET-SAFE.

# # #

News Release

For further information:

Jon Mellor, AT&T
908-221-5017 (office)
908-874-8964 (home)

HOSPITALS FALL PREY TO TELEPHONE FRAUD

FOR IMMEDIATE RELEASE

BASKING RIDGE, N.J. -- Is your switchboard an open door to thieves who will steal your long-distance service? AT&T warns that hospitals are increasingly targeted in slick scams that cost everyone money.

"Administrators should be aware of the threat posed by con artists. They will stop at nothing to get a receptionist or switchboard operator to give them access to long-distance lines," said Richard Petillo, director-AT&T Corporate Security.

Two scams have been "making the rounds" recently at hospitals. Both take advantage of the victims' eagerness to be helpful.

- more -

In one, a caller posing as an AT&T technician or security officer calls the hospital's main number. The caller asks the receptionist to help in an investigation by saying "yes" when an "operator" calls to verify third-party charges. The scammer assures the receptionist that the hospital won't be charged for the calls. But it will, and the calls are generally expensive international calls that can add up to thousands of dollars.

In another ploy, a "Dr. X" makes a collect call to the hospital, and asks to be transferred to "Dr. Y." (Crooks can easily get the names of actual doctors who practice at specific hospitals.) He may ask to be transferred one or more times before asking to be transferred back to the receptionist, and he then asks for an outside line. Once he gets it, he may make unlimited calls. Again, the hospital is fully liable.

Con artists will always look for ways to steal long-distance service, but some simple steps can help save a hospital from fraudulent charges:

- o Never accept a collect call from anyone identifying himself or herself as a phone-company employee.
- o No one from a reputable telephone company would ever ask to charge calls to another number, for any reason.
- o AT&T and other telephone companies do not ask their customers to help trap criminals or to help with line problems or any kind of maintenance procedure.
- o Never accept third-party charges from, or provide an outside line to, an unknown person.

An administrator who suspects fraud should call the hospital's long-distance telephone company. AT&T can be reached at 1-800-CALL-ATT. Organizations and government agencies that can assist victims and provide other preventive tips include: the National Fraud Information Center, 1-800-876-7060; the Better Business Bureau; and the Federal Trade Commission, 202-326-2402.

###

News Release

For further information:

Mitchel Montagna
904-954-8896 (office)
904-646-3270 (home)

Claire Diamond
904-954-7175 (office)
904-367-0627 (home)

CONSUMERS CAN TAKE A BITE OUT OF CREDIT CARD FRAUD

FOR RELEASE MONDAY, OCTOBER 18, 1993

JACKSONVILLE, Fla. -- Heavy credit card usage increases the likelihood of fraud. But as consumers look forward to the holiday season, they should know that by following a few basic rules, they are in a much better position to protect their accounts.

"Immediate consumer action is the crook's worst nightmare," said Rick Brady, a loss-prevention manager at AT&T Universal Card Services. "If your card is lost or stolen, report it immediately to the issuer. Most are open 24 hours a day, seven days a week."

Brady also counsels people to beware of telemarketing fraud. It affects consumers more than other types of fraud because the cardholder is not immediately aware he is the victim of a crime.

Telemarketing fraud means a con artist calls a consumer under a false pretext -- pretending to be, for example, a local retailer or utility company -- and claims to need the cardmember's credit card account or personal identification number (PIN).

- more -

"Never give your account number or PIN to someone calling you," Brady said. "You don't know who they really are."

Brady offers other anti-fraud tips for consumers:

- o Verify that your statement matches your receipts.
- o Never write your PIN on your card or have it in your wallet.
- o Keep all your credit card account numbers written in a safe place away from your cards.

Brady adds that now is an especially good time to keep these hints in mind. The United States Office of Consumer Affairs has designated the week of October 24 as National Consumers Week. This year The Office urges organizations across the country to focus their educational efforts on preventing fraud.

# # #

AT&T HELPS CONSUMERS AVOID FRAUD;

PROMOTES NATIONAL CONSUMERS WEEK

DATELINE--The telephone is an integral part of our daily lives. It keeps us in touch with those we love, provides a lifeline to essential services and enables companies to do business with each other around the world.

It also is a vehicle for a variety of fraudulent schemes which cost U.S. taxpayers and businesses from $3 billion to $40 billion each year.

According to Richard Petillo, corporate security manager for AT&T, the two groups targeted most frequently by scam artists are senior citizens and recent immigrants to the U.S. As part of National Consumers Week (October 24-30), AT&T offers the following tips to help consumers protect themselves from falling prey to various fraud schemes.

- Never respond to an unsolicited offer for goods or services by giving a credit card number. Ask that printed information be mailed to you. Also, research the company before giving it any kind of payment.
- Never give a personal or business credit card number to anyone unless you're certain the request is legitimate. Don't ever give a credit card number as a means of identification.

-more-

- Never reveal a long distance calling card number to anyone. The only time a telephone company representative will ask for your calling card number is when YOU initiate an operator-assisted call.
- When using a public phone, look around before giving a calling card number to an operator. Block the view of the keypad when dialing a card number. Keep your telephone card out of sight range -- "shoulder surfers" have been known to memorize numbers while callers are using cards at pay phones.
- Never accept third-party charges from someone you don't know. Telephone company representatives do not ask to charge calls to your home.
- If you are a business owner and you provide your employees with corporate calling cards, make sure the company that issues the cards offers a security package. For example, AT&T Card Protect (sm) includes a written guarantee that states if its cards are lost or stolen, businesses won't pay for fraudulent calling card calls made by people they don't know.
- If the sales pitch includes any of the following phrases, be careful: "You've been specially selected to hear this offer." "You'll get a wonderful free bonus if you buy our product." "You've won a valuable free prize." "You have to make up your mind right away."

-more-

Petillo says phone fraud scam artists use well-rehearsed sales pitches that sound very believable. "Potential victims may even be transferred from one person to another to make the call appear to be valid. People should always be wary of high-pressure sales tactics that require an immediate decision. Legitimate companies always give people time to think things over," he says.

Most victims of telephone and telemarketing fraud lose their money, discover the investment they were told about was non-existent or never receive the free gift they were promised. Many also find massive telephone charges on their long-distance calling-card statements or discover unauthorized charges appearing on their credit card bills.

"The most important thing to do if you find yourself a victim of fraud is to report it," Petillo says. "Many people are embarrassed to fall for a scheme and they don't want others to know. Unfortunately, it just allows the crooks to keep on scamming others."

To help law enforcement personnel catch the perpetrators, victims should save all documents, including postcards, canceled checks, telephone bills, credit card statements, etc. It also helps to keep detailed notes of telephone conversations, including dates, times and names, if possible.

-more-

Finally, if any part of the fraudulent transaction took place through the U.S. Postal Service (including receipt of literature or mailing of a payment) contact the local postal inspector immediately. The U.S. Postal Inspection Service pursues both civil and criminal prosecution when the mail is used as an integral part of a scheme to defraud.

AT&T also offers a free brochure, "Be Aware of Phone Fraud." To get a copy, call toll free on 1-800-851-0439.

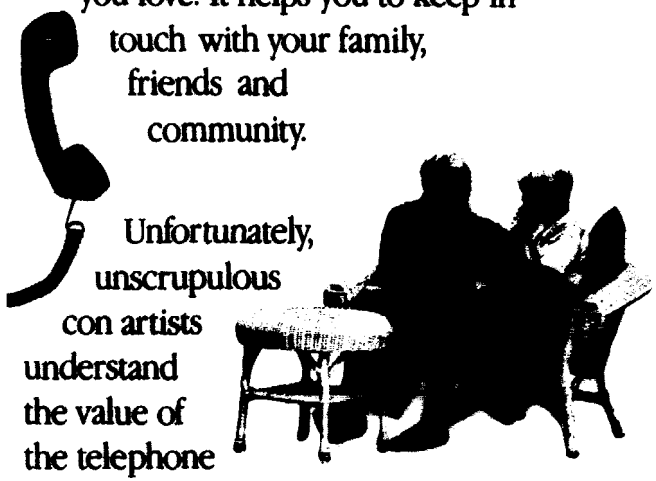
-0-

Be Aware.

Don't be a victim of phone fraud.

PHONE FRAUD ALERT

We know it may be hard to believe that your telephone could be used against you. After all, no matter where you are, the telephone connects you with the people you love. It helps you to keep in touch with your family, friends and community.



Unfortunately, unscrupulous con artists understand the value of the telephone as well. For them, the telephone is an easy, accessible vehicle for conducting a wide variety of schemes such as fraudulent third-party charges, calling card frauds and bogus investment plans, just to mention a few.

The good news is that you can avoid becoming a victim of phone fraud. Once you are aware that there are people who use the phone lines to deceive others, you will instinctively listen more carefully. And, even though con artists are very good at what they do, they are no threat if you are informed and alert.

SCAM: Accepting toll charges for third-party calls

Your natural instincts to be a good citizen may well entrap you in this costly scam. Here's how it works: Someone will call and identify himself as a representative of the telephone company. He will request your assistance in an investigation by asking you to say "yes" when the operator calls to verify third-party charges (for toll calls made by someone else and charged to your number) for a specific period of time. And, he will assure you that you will not be charged for these calls. If you hesitate or seem reluctant to cooperate, he may even tell you that your telephone service will be terminated, or that you will have to pay for all fraudulent calls charged to your phone.

Defense:

- No one from the telephone company would ever ask to charge calls to your home.
- Never accept third-party charges from anyone you don't know.
- You can be sure that AT&T and other long distance and local telephone companies do not enlist the assistance of their customers to trap telephone con artists.

SCAM: Revealing your calling card number

Your calling card number is like money in the bank to a scam artist who will use it to sell discounted long distance calls to locations around the world. There are any number of schemes that he will use to get your number from you. Two favorites are:

When you are making a call from a public phone, the thief may linger close by in order to hear you reveal your calling card number to the operator. He may also watch as you dial your card number.

Someone may call you at home and, posing as a telephone representative, ask for your calling card number to check on unauthorized charges, or to help trap a telephone scam artist.

Defense:

- When using a public telephone, look around before you give your calling card number to the operator. Speak directly into the mouthpiece in a quiet voice. Block the view of the keypad when you dial your calling card number. Whenever possible, look for a public phone that magnetically reads your calling card.
- No telephone company representative will ever ask you for your calling card number unless you are actually initiating an operator-assisted calling card call.

SCAM: Participating in bogus investment schemes

Phony investment counselors will call to urge you to invest in a wide range of too-good-to-be-true deals–anything from precious metals, to oil and gas drilling, foreign currencies, penny stocks, time-share condominiums and more. They will invariably offer you high profits, low risk and tell you that you must act immediately to get in on the deal. Remember, they are trained to be articulate, forceful and believable.

Defense:

◀ Your best defense is to simply hang up when you suspect you're being conned, or to ask relevant questions like:

–Where did you get my name? (Do not accept "from a special list.")
–Where will the money be held?
–What type of written statement do you provide?

◀ Always ask the caller to send you a brochure or other printed materials. Con artists will usually hang up when they realize that you are not an easy prey.

◀ Remember, there are also many legitimate telemarketers who are always willing to answer questions, send you information and give you time to make up your mind.

SCAM: Purchasing phony vacation packages

Other callers will entice you with promises of a wonderful vacation priced far below market value. You are asked to make the reservation with your credit card. However, the trip may be subject to major restrictions, postponed frequently or cancelled.

If you do get to go, you will probably end up in a rundown hotel spending more money on additional charges than you would have if you had bought the trip from a legitimate travel agent. Worst of all, unauthorized charges may begin to appear on your credit card statement.

Defense:

◀ Never respond to such an offer by giving your credit card number. Ask that additional information be sent to you.

SCAM: Disclosing your consumer credit card number

A caller will ask for your consumer credit card number in order to send you a prize or a product you haven't ordered, verify an insurance policy or check charges on your credit card account.

Defense:

◀ Never give your consumer credit card number to anyone unless you are absolutely certain that the request is legitimate–for example, you are ordering a product from a catalogue or making a hotel reservation. Do not reveal your credit card number simply as a means of identification.